

IC CARD, IC CARD AUTHENTICATION SYSTEM AND ITS AUTHENTICATION METHOD

Publication Number: 2001-126046 (JP 2001126046 A) , May 11, 2001

Inventors:

- ☐ HARUMOTO MASAHIRO
- ☐ DEGUCHI TOSHIKI

Applicants

- ☐ KYODO PRINTING CO LTD

Application Number: 11-308256 (JP 99308256) , October 29, 1999

International Class:

- ☐ G06K-019/10
- ☐ B42D-015/10
- ☐ G06K-017/00
- ☐ G06K-019/08
- ☐ G06T-001/00
- ☐ G09C-001/00
- ☐ G09C-005/00
- ☐ H04N-001/387

Abstract:

PROBLEM TO BE SOLVED: To provide an IC card, and IC card authentication system/method, which discriminate the rightness of the IC card and can suppress forgery and duplication. **SOLUTION:** An IC card 100 being an execution form has an IC chip 11 storing first authentication information and a face photograph information 12 where second authentication information is buried in a face photograph for recognizing a card possessor on a card base material 1. Since electronic transparent information as second authentication information can be buried in picture data of face photograph information 12 in a non-visible state and is concealed, even the card possessor cannot recognize second authentication information by eyes. The authentication information is read by using a prescribed reader and compared/judged. Thus, the rightness of the card and that of the user can be recognized. Then, effect for braking and suppressing forgery and duplication is attained. **COPYRIGHT:** (C) 2001, JPO

JAPIO

© 2004 Japan Patent Information Organization. All rights reserved.
Dialog® File Number 347. Accession Number 6898536

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-126046

(P2001-126046A)

(43) 公開日 平成13年5月11日 (2001.5.11)

(51) Int.Cl. ⁷	識別記号	F I	テームト [*] (参考)
G 0 6 K 19/10		B 4 2 D 15/10	5 2 1 2 C 0 0 5
B 4 2 D 15/10	5 2 1	G 0 6 K 17/00	T 5 B 0 3 5
G 0 6 K 17/00		G 0 6 T 1/00	5 0 0 B 5 B 0 5 7
19/08		G 0 9 C 1/00	6 6 0 A 5 B 0 5 8
G 0 6 T 1/00	5 0 0	5/00	5 C 0 7 6

審査請求 未請求 請求項の数11 OL (全 8 頁) 最終頁に続く

(21) 出願番号 特願平11-308256

(22) 出願日 平成11年10月29日 (1999. 10. 29)

(71) 出願人 000162113

共同印刷株式会社

東京都文京区小石川4丁目14番12号

(72) 発明者 春本 昌宏

東京都文京区小石川四丁目14番12号 共同
印刷株式会社内

(72) 発明者 出口 俊樹

東京都文京区小石川四丁目14番12号 共同
印刷株式会社内

(74) 代理人 100084250

弁理士 丸山 隆夫

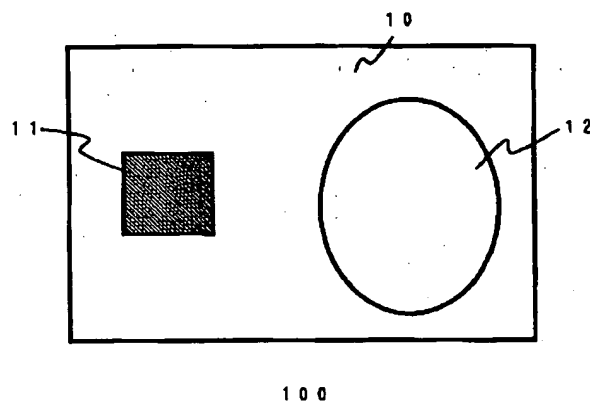
最終頁に続く

(54) 【発明の名称】 ICカード、ICカード認証システム、及びその認証方法

(57) 【要約】

【課題】 ICカードの正当性を判別でき、偽造及び複製を抑止することのできるICカード、ICカード認証システム及びその認証方法を提供する。

【解決手段】 本発明の実施形態であるICカード100は、カード基材1上に、第1の認証情報を記憶したICチップ11と、カード所有者を認識するための顔写真に第2の認証情報が埋め込まれた顔写真情報12と、を備えている。この第2の認証情報としての電子透かし情報は、顔写真情報12の画像データに不可視状態で埋め込み隠匿させることができるので、通常、カード所有者であっても第2の認証情報を目視により確認することができない。従って、これらの認証情報を所定の読み出し装置を用いて読み出して比較判定することにより、カードの正当性および使用者の正当性を確認することができ、偽造及び複製に対し多に牽制並びに抑止する効果を得ることができる。



【特許請求の範囲】

【請求項1】 少なくとも第1の認証情報を記憶したICチップを内蔵したカード基材と、
前記カード基材の表面に第2の認証情報を埋め込んだ少なくとも画像や幾何学模様、図形および線画から選択される画像情報を設けたことを特徴とするICカード。

【請求項2】 前記画像情報は、前記第1の認証情報と前記第2の認証情報とを照合することにより正当性を認証することが可能な情報からなることを特徴とする請求項1記載のICカード。

【請求項3】 前記第1の認証情報及び前記第2の認証情報は、
少なくとも文字、数字、図形や前記画像情報と直接関連するサインから選択されるいずれか1つの情報、あるいは、それらを組み合わせた情報から生成されていることを特徴とする請求項1または2記載のICカード。

【請求項4】 前記画像情報が画像の場合には、
少なくとも画素置換方法、画素空間利用方法、量子化誤差利用方法、統計利用方法や離散フーリエ変換方法（FFT）、離散コサイン変換方法（DCT）、ウェーブレット変換方法（WLT）、スペクトラム拡散方法（SS）による周波数領域利用方法、及びクロミナンス成分利用方法、ルミナンス成分利用方法、エッジ利用方法から選択された方法を用いた電子透かし技術により前記第2の認証情報が前記画像情報に埋め込まれていることを特徴とする請求項1から3のいずれか1項に記載のICカード。

【請求項5】 前記画像情報が模様の場合には、
少なくともスペーシング利用法、回転／伸縮利用法、コード利用法や代替文字利用法から選択された方法を用いた電子透かし技術により前記第2の認証情報が前記画像情報に埋め込まれていることを特徴とする請求項1から3のいずれか1項に記載のICカード。

【請求項6】 前記画像情報は、二値画像または多値画像のいずれかの情報であることを特徴とする請求項1から5のいずれか1項に記載のICカード。

【請求項7】 前記画像情報は、前記カード基材上に形成され、ICカードの所有者を表す認証用の顔画像、該ICカードの出所を示すマークや該カード基材上に形成された模様であることを特徴とする請求項1から6のいずれか1項に記載のICカード。

【請求項8】 少なくとも第1の認証情報を記憶したICチップと第2の認証情報を埋め込んだ前記画像情報とを備えるICカードと、該ICカードにおける前記第1の認証情報及び前記第2の認証情報の各々を読み取る読み取り装置からなるICカード認証システムであって、
前記読み取り装置は、
前記ICチップに記憶されている前記第1の認証情報を読み取る第1の読み取り手段と、
前記画像情報に埋め込まれている前記第2の認証情報を

読み取る第2の読み取り手段と、

前記第1の読み取り手段により読み取られた前記第1の認証情報と前記第2の読み取り手段により読み取られた前記第2の認証情報とを照合することにより正当か否かを判定する判定手段と、
を有することを特徴とするICカード認証システム。

【請求項9】 前記読み取り装置は、
前記第1の読み取り手段により読み取られた前記第1の認証情報を表示する第1の表示手段と、
前記第2の読み取り手段により読み取られた前記第2の認証情報を表示する第2の表示手段と、
前記判定手段による判定結果を表示する第3の表示手段と、
を有することを特徴とする請求項8記載のICカード認証システム。

【請求項10】 前記ICカード認証システムは、
前記第1の認証情報を前記ICチップに記憶する記憶手段と、
前記第2の認証情報を埋め込んだ前記画像情報を前記カード基材の表面に設ける画像情報形成手段と、
を有することを特徴とする請求項8記載のICカード認証システム。

【請求項11】 少なくとも第1の認証情報を記憶したICチップと第2の認証情報を埋め込んだ前記画像情報とを備えるICカードと、該ICカードにおける前記第1の認証情報及び前記第2の認証情報の各々を読み取る読み取り装置からなるICカード認証システムを用いたICカードの認証方法であって、
前記ICチップに記憶されている前記第1の認証情報を読み出す第1の読み出し工程と、
前記画像情報に埋め込まれている前記第2の認証情報を読み出す第2の読み出し工程と、
前記第1の読み出し工程により読み出された前記第1の認証情報と前記第2の読み出し工程により読み出された前記第2の認証情報とを照合することにより正当か否かを判定する判定工程と、
を有することを特徴とするICカードの認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ICカード、ICカード認証システム及びその認証方法に関し、特に第三者により該ICカードの所有者を表す認証用の顔画像の偽造、複製及び改ざん等を防止または抑制するための情報を備えるICカード、ICカード認証システム及びその認証方法に関する。

【0002】

【従来の技術】 現代社会において、カードの使用及び当該カードを用いてシステムを利用するといった機会が非常に多くなってきている。例えば、このようなカードとしては、会社等で用いられる社員証用のIDカード、金

融機関により発行されるキャッシュカードや各種金融機関により発行されるクレジットカード等がそうである。

【0003】上記カード及びカードを用いたシステムにおいては、カードの真偽性、すなわち、カードが正当に発行されたものであるか否か、カードの使用者が正当なカード所有者であるか否か、または、カードに記憶されている情報が改ざんされているか否か、といった点が大変重要になってくる。

【0004】例えば、カードの正当な使用者から何らかの理由により不正に第三者が当該カードを入手し、このカードに記憶されている情報を使用した場合、正当なカード所有者が多大な被害をこうむることになる。このことは、単に個人レベルの問題としてでなく、カードの社会的信用性にも係わる大きな問題である。

【0005】上述されるような問題を解決する方法として、最近では使用者の顔写真をカード上に形成し、カードが使用される際に当該カードの使用者とカード上に形成された顔写真とを目視により比較確認し、カードの使用者が正当なカード所有者であるか否かを判別することが行われている。

【0006】しかしながら、この方法においては、不正にカードを入手した第三者が顔写真を削り取る等して、第三者の顔写真にすげ替え、あたかも正当なカード所有者であるかのごとくカードを使用するといった不正が行われる可能性がある。

【0007】これは、クレジットカードの加盟店において、少額の取引の場合には、クレジットカード認証端末装置を用いずに該カードの写真情報を担当者が確認することのみで決済することも日常的に行われていることを利用し、第三者が不正に使用することができるといった問題である。

【0008】また、従来のカードにおいては、該カードの情報は、磁気ストライプに記録されているものが主流であるが、この磁気ストライプに記録されている情報は、比較的容易に改ざんされる可能性があり、セキュリティ面における問題がある。

【0009】このセキュリティ面の問題を解消するものとして、ICカードが知られている。このICカードにおける最大の利点は、該カードに内蔵されたICチップに記憶されている情報の改ざんが困難であると共に、ICチップに記憶することのできる情報蓄積量の多さといった点にある。

【0010】このようなICカードの利点と上述される顔写真とを組み合わせ、カード所有者の正当性を容易に確認でき、また、ICチップに記憶されている情報の改ざんの困難性を持ち合わせたものとして、例えば、特開平4-271494号公報に開示されるような「ICカード」がある。

【0011】このICカードは、データ処理用のCPUと、プログラム格納用のROMデータ格納用EEPROM

Mと、外部とのデータのやり取りを行うI/O装置とを有して構成される写真付きICカードである。ICカード上に設けられた写真のイメージ情報をEEPROM内に格納しておき、例えば、カード所有者の入退室時において、所定の読み出し装置によりEEPROM内に格納されている写真のイメージ情報を読み出し、I/O装置を介して併設されるモニタ上に当該イメージ情報を映し出す。このことにより、ICカード上に設けられた写真、モニタ上に映し出された写真のイメージ情報、ICカードの使用者本人、のそれぞれを認証者が目視により比較することで該カードの使用者が正当なICカードの所有者であるか否かを認証するようにしたものであった。

【0012】

【発明が解決しようとする課題】しかしながら、上記従来例においては、ICカード上に設けられている写真情報を削り取る等の手段により消去し、その消去した箇所に第三者が写真情報を形成することで、写真情報のすげ替えただけで不正にカードを第三者が使用することができるといった可能性があった。

【0013】また、情報処理機器の発達により一部のマニアが、写真情報をすげ替えるだけではなく、ICカードに内蔵されているICチップに記憶された写真情報を書き換える可能性があり、この場合には、上述の方法により読み出してカードの使用者を比較検討した場合、ICカードが偽造されたものであるか否かが判断できないといった問題があった。

【0014】本発明は、上述されるような問題を解決するために成されたものであり、ICカード上に設けられている写真情報をすげ替えるだけではなく、ICカードに内蔵されているICチップに記憶された写真情報を書き換えられ、ICカードが改ざんされた場合であっても、容易にその改ざんによる不正を判別できると共に、改ざん及び複製を抑止することのできるICカード、ICカード認証システム及びその認証方法を提供することを目的とする。

【0015】

【課題を解決するための手段】前記課題を解決するために、請求項1記載の発明は、少なくとも第1の認証情報を記憶したICチップを内蔵したカード基材と、カード基材の表面に第2の認証情報を埋め込んだ少なくとも画像や幾何学模様、図形および線画から選択される画像情報を設けたことを特徴とする。

【0016】請求項2記載の発明は、請求項1記載の発明において、画像情報は、第1の認証情報と第2の認証情報とを照合することにより正当性を認証することが可能な情報からなることを特徴とする。

【0017】請求項3記載の発明は、請求項1または2記載の発明において、第1の認証情報及び第2の認証情報は、少なくとも文字、数字、図形や画像情報と直接関

連するサインから選択されるいずれか1つの情報、あるいは、それらを組み合わせた情報から生成されていることを特徴とする。

【0018】請求項4記載の発明は、請求項1から3のいずれか1項に記載の発明において、画像情報が画像の場合には、少なくとも画素置換方法、画素空間利用方法、量子化誤差利用方法、統計利用方法や離散フーリエ変換方法（FTT）、離散コサイン変換方法（DCT）、ウェーブレット変換方法（WLT）、スペクトラム拡散方法（SS）による周波数領域利用方法、及びクロミナンス成分利用方法、ルミナンス成分利用方法、エッジ利用方法から選択された方法を用いた電子透かし技術により第2の認証情報が画像情報に埋め込まれていることを特徴とする。

【0019】請求項5記載の発明は、請求項1から3のいずれか1項に記載の発明において、画像情報が模様の場合には、少なくともスペーシング利用法、回転／伸縮利用法、コード利用法や代替文字利用法から選択された方法を用いた電子透かし技術により第2の認証情報が画像情報に埋め込まれていることを特徴とする。

【0020】請求項6記載の発明は、請求項1から5のいずれか1項に記載の発明において、画像情報は、二値画像または多値画像のいずれかの情報であることを特徴とする。

【0021】請求項7記載の発明は、請求項1から6のいずれか1項に記載の発明において、画像情報は、カード基材上に形成され、ICカードの所有者を表す認証用の顔画像、該ICカードの出所を示すマークや該カード基材上に形成された模様であることを特徴とする。

【0022】請求項8記載の発明は、少なくとも第1の認証情報を記憶したICチップと第2の認証情報を埋め込んだ画像情報とを備えるICカードと、該ICカードにおける第1の認証情報及び第2の認証情報の各々を読み取る読み取り装置からなるICカード認証システムであって、読み取り装置は、ICチップに記憶されている第1の認証情報を読み取る第1の読み取り手段と、画像情報に埋め込まれている第2の認証情報を読み取る第2の読み取り手段と、第1の読み取り手段により読み取られた第1の認証情報と第2の読み取り手段により読み取られた第2の認証情報とを照合することにより正当か否かを判定する判定手段と、を有して構成されることを特徴とする。

【0023】請求項9記載の発明は、請求項8記載の発明において、読み取り装置は、第1の読み取り手段により読み取られた第1の認証情報を表示する第1の表示手段と、第2の読み取り手段により読み取られた第2の認証情報を表示する第2の表示手段と、判定手段による判定結果を表示する第3の表示手段と、を有することを特徴とする。

【0024】請求項10記載の発明は、請求項8記載の

発明において、ICカード認証システムは、第1の認証情報をICチップに記憶する記憶手段と、第2の認証情報を埋め込んだ画像情報をカード基材の表面に設ける画像情報形成手段と、を有することを特徴とする。

【0025】請求項11記載の発明は、少なくとも第1の認証情報を記憶したICチップと第2の認証情報を埋め込んだ画像情報とを備えるICカードと、該ICカードにおける第1の認証情報及び第2の認証情報の各々を読み取る読み取り装置からなるICカード認証システムを用いたICカードの認証方法であって、ICチップに記憶されている第1の認証情報を読み出す第1の読み出し工程と、画像情報に埋め込まれている第2の認証情報を読み出す第2の読み出し工程と、第1の読み出し工程により読み出された第1の認証情報と第2の読み出し工程により読み出された第2の認証情報とを照合することにより正当か否かを判定する判定行程と、を有することを特徴とする。

【0026】

【発明の実施の形態】次に、添付図面を参照して本発明に係るICカード、ICカード認証システム及びその認証方法を図1から図3を用いて以下に説明する。

【0027】図1は、本発明の実施形態であるICカードの外観を示す平面図である。図1において、本発明の実施形態であるICカード100は、カード基材10上に、第1の認証情報を記憶したICチップ11と、カード所有者を認識するための顔写真に第2の認証情報として該カード所有者のサインが埋め込まれた顔写真情報12と、を備えている。

【0028】なお、この顔写真情報12は、二値（白黒）画像、多値（カラー）画像の何れであってもよい。また、顔写真に代えてカード基材10上の幾何学模様、図形および線画等の模様でカード所有者を認識するための該カード所有者のサインを第2の認証情報として埋め込むこともできる。

【0029】本発明の第2の認証情報として用いられている電子透かし情報は、例えば、顔写真情報12等の画像データに不可視状態で埋め込み隠匿させることができるので、カード所有者であっても、通常の状態において第2の認証情報を目視により確認することができず、また、顔写真に代えてカード基材10上の幾何学模様、図形および線画等の模様でカード所有者を認識するための該カード所有者のサインを第2の認証情報として埋め込むことができる。

【0030】また、電子透かし情報が埋め込まれた顔写真情報12の顔写真から第三者が電子透かし情報を取り出す場合には、該顔写真情報12が破壊されてしまい、顔写真情報12に別の電子透かし情報を書き換えることが非常に困難である。

【0031】以上のような特性を備える電子透かし情報を顔写真に埋め込む方法として、以下に示される方法が

ある。

【0032】モノクロ顔写真等のモノクロ画像データに電子透かし情報を埋め込む方法として、第1の方法としては、画素のビット情報を密かに電子透かし情報用のビット情報に置き換える画素置換方法がある。この場合、画素位置におけるどのビット情報を置換するかを鍵として指定するものである。

【0033】また、第2の方法としては、対象となる画素の近傍3×3画素の平面を輪切りにして取り出し、この周囲8ビットに対して署名印などを埋め込む画素空間利用方法がある。この場合、原画の1/3の電子透かし情報を256階調で秘匿することができる。

【0034】また、第3の方法として、モノクロ画像データの圧縮時において、次入力画素から既に入力画素の予測値で差分を求め、その結果を量子化して符号化するために用いられる量子化誤差に注目し、電子透かし情報のビット系列の0、1で量子化出力 Δ_i を偶数と奇数に制御することで、見かけ上、量子化ノイズとして電子透かし情報を埋め込む量子化誤差利用方法がある。

【0035】また、第4の方法として、モノクロ画像データの周波数領域に電子透かし情報を埋め込む周波数領域利用方法がある。この場合、圧縮、拡大、回転、微分、平滑化、切断等の各種の画像処理、特に、モノクロ画像データを蓄積し、伝送する際に画像圧縮をすると、埋め込まれた電子透かし情報のデータが散逸してしまい、完全に符号化できないといった問題を回避することができる。このような周波数領域利用方法としては、例えば、離散フーリエ変換法(FTT)、離散コサイン変換法(DCT)、ウェーブレット変換法(WLT)、スペクトラム拡散法(SS)等がある。

【0036】さらに、第5の方法として、モノクロ画像データの濃淡におけるn個の任意の画素値に偏り+ Δ を与え、さらにn個の任意の画素値に偏り- Δ を与えて戻す統計利用方法である。この場合、繰り返し数や偏りの設定を適当に選ぶことにより耐久性のある方法として用いられ、パッチワークと称されるものである。

【0037】次に、カラー顔写真等のカラー画像データに電子透かし情報を埋め込む方法を以下に示す。カラー画像データは、モノクロ画像データに比べて非常に大きい冗長性を有しており、カラー画像における明度、色相、彩度を利用して、人間の目に識別できない範囲内でカラー画像データ中に電子透かし情報を埋め込むことができるからである。

【0038】このカラー画像データに電子透かし情報を埋め込む第1の方法として、人間の視覚特性において、色差情報や彩度情報は、一般に輝度情報よりも階調識別能力が低下するという点を利用し、高周波色差情報を用いて画質を劣化することなく電子透かし情報を読み込むといったクロミナンス成分利用方法がある。

【0039】また、第2の方法として、カラー画像デー

タのルミナンス成分(Y)と、クロミナンス成分

(C_r , C_b)とに分離した後、JPEGのアルゴリズムに基づいて、二次元離散コサイン変換を実行し、この時、Y成分に対して変換出力をJPEG指定により量子化すると量子化誤差が発生するので、この量子化誤差を利用して電子透かし情報を埋め込むルミナンス成分利用方法がある。

【0040】さらに、第3の方法として、カラー画像データにおいては、輝度成分の平坦部分と変化の著しい部分(エッジ)とが存在し、人間の視覚特性としてこの平坦部分におけるノイズに対して比較的鈍感であるという点を利用し、その画像のエッジ部分にのみ集中して画素情報を電子透かし情報に置換、または、変調するエッジ利用方法がある。

【0041】なお、顔写真などの画像情報ではなく、幾何学模様、図形および線画等の模様文字、数字、図形やサイン等の電子透かし情報を埋め込む場合には、ポストスクリプト(Postscript)を用い、例えば、英文の単語と単語との間の区切り符号としての空白部分を利用したスペーシング利用法、和文等の字画が多い場合には、文字を少し回転させたり、活字ポイントを僅かに下げたりして前後左右の文字との設定の差を利用した回転/伸縮利用法、地紋などの図形の空白にバーコード等を疑似化(粉飾化)して利用するコード利用法や単語の一部または全部を意図的に置き換えたり、文書構造を利用したりする代替文字利用法を用いることができる。

【0042】本発明の実施形態において、顔写真にカード所有者のサインからなる電子透かし情報を顔画像情報12に埋め込む方法としては、上述されるいずれの方法を用いても可能である。

【0043】また、顔画像情報12に埋め込む電子透かし情報として用いる情報は、特に限定されるものでなく、このような文字、数字、図形や画像情報と直接関連するサイン等を暗号化したものを第2の認証情報として用いることも可能である。

【0044】さらに、電子透かし情報として入力されるデータは、8ビット程度で構成されるものでもよく、埋め込まれる顔画像情報12に影響を与えず、また、電子透かし情報の読み出し時における処理速度が低下するといった問題もなく、短時間で判定を行うことができる。

【0045】図2は、本発明の実施形態であるICカード認証システムの概略構成を示す図である。図2において、本発明の実施形態であるICカード認証システムは、図1に示されるICカード100と、読み取り装置200と、により構成され、読み取り装置200の制御部24に入力部27及びプリンタ300を別途接続することで、ICカード100を発行することもできる。

【0046】まず、読み取り装置200の制御部24に入力部27及びプリンタ300を接続したICカード認証システムにICカードを挿入する。このICカード

は、情報が記録されていないＩＣカード（図示しない）である。

【００４７】このＩＣカードのカード基材１０上に、テンキー等の入力部２７からカード所有者のサインのスペルを第１の認証情報としてＩＣチップ１１に記憶し、カード所有者を認識するための顔写真に第２の認証情報として該カード所有者のサインが埋め込まれた顔写真情報１２をプリンタ３００で記録する。

【００４８】その具体的な方法としては、まず、カード所持者の顔写真に第２の認証情報として該カード所有者のサインのスペルに該当する文字列をテンキーなどの入力部２７から入力し、制御部２４でＪＩＳコード（２バイトの二進数化）を「０１００１１０１０００・・・」のように二進化し、記憶部２６に記憶する。

【００４９】次に、カード所持者の顔写真をスキャナ２２により読み込み、この顔写真を各色の値が０から２５５階調の値となるように制御部２４で二進化し、記憶部２６に記憶する。このとき、顔写真は「０」と「１」に対応させた写像を $y=f(x)$ において、 $f:x \bmod 2$ （ \bmod は、除算の余りを求める演算子）となるようにし、任意の位置（点）の色情報を「０」もしくは「１」に対応させる。

【００５０】次に、記憶部２６に記憶されている二進化された顔写真と、この顔写真に電子透かし情報として埋め込む第２の認証情報であるカード所有者のサインのスペルに該当する文字列を２バイトの二進数化した「０１００１１０１０００・・・」を読み出し、制御部２４において、二進化された顔写真の任意の位置の画素から順に１ビットの情報を１つの点に対応させ、画素値が埋め込む二進数と一致していればそのままの画素値を採用し、一致しなければ画素値の変更を行い新しい画素とするクロミナンス成分利用法を用いて、顔写真に第２の認証情報であるカード所有者のサインを埋め込んだ画像情報を作成し、この画像情報をプリンタ３００によりＩＣカードのカード基材１０上に顔写真情報１２として記録し、ＩＣカード１００とする。

【００５１】本発明の実施形態であるＩＣカード認証システムは、図１に示されるＩＣカード１００と、図２の読み取り装置２００により構成され、読み取り装置２００は、ＩＣプローブ２１と、スキャナ２２と、透かし情報抽出部２３と、制御部２４と、表示部２５と、記憶部２６と、入力部２７と、から構成される。

【００５２】ＩＣプローブ２１により、接触形式または非接触形式を問わず、ＩＣカード１００に設けられたＩＣチップ１１に記憶されている第１の認証情報を読み出し、制御部２４に送出する。

【００５３】スキャナ２２は、ＩＣカード１００表面に形成される顔写真情報１２を読み取り、二値化画像に変換して透かし情報抽出部２３へ送出する。

【００５４】透かし情報抽出部２３は、スキャナ２２か

ら送られた顔写真情報１２の二値化画像に埋め込まれている第２の認証情報であるカード所有者のサインのスペルに該当する文字列を２バイトの二進数化した「０１００１１０１０００・・・」を抽出し、制御部２４へ送出する。

【００５５】制御部２４は、ＩＣプローブ２１により読み出された第１の認証情報であるカード所持者のサインのスペルと、第２の認証情報である透かし情報抽出部２３により抽出されたカード所有者のサインのスペルに該当する文字列を２バイトの二進数化した「０１００１１０１０００・・・」と電子透かし情報とが一致するかどうかを判定する。なお、制御部２４は、図示されないＲＯＭに記憶されている制御プログラムに基づいて、読み取り装置２００全体の動作制御を司る。

【００５６】表示部２５は、ＩＣプローブ２１により読み出された第１の認証情報であるカード所持者のサインのスペルと、透かし情報抽出部２３により抽出された第２の認証情報である電子透かし情報と、制御部２４により判定された結果とを表示するものである。

【００５７】また、読み取り装置２００にスピーカを設け、制御部２４により判定された判定結果を当該スピーカを鳴動させることにより、報知するように構成することも可能である。

【００５８】図３は、本発明の実施形態であるＩＣカード認証システムにおける認証動作の一例を示すフローチャートである。図３において、まず、読み取り装置２００にＩＣカード１００が載置されると（ステップＳ１）、ＩＣチップ１１に記憶されている第２の認証情報をＩＣプローブ２１により読み出し、当該読み出された第２の認証情報を制御部２４に送出する（ステップＳ２）。

【００５９】次に、ＩＣカード１００上に印刷等により形成されている顔写真情報１２をスキャナ２２により読み取り、それを二値化画像に変換して透かし情報抽出部２３へ送出する（ステップＳ３）。

【００６０】透かし情報抽出部２３は、スキャナ２２からの二値化画像から所定の処理に基づいて電子透かし情報を抽出し、当該抽出された電子透かし情報を制御部２４に送出する（ステップＳ４）。

【００６１】制御部２４は、ＩＣプローブ２１から送出された第１認証情報と、透かし情報抽出部２３から送出された第２の認証情報とが一致するかどうかを判定し、当該判定結果を表示部２５へ出力する（ステップＳ５）。

【００６２】表示部２５は、制御部２４から出力された判定結果を表示画面上に表示する（ステップＳ６）。

【００６３】なお、本発明では、第１の認証情報および第２の認証情報にカード所持者のサインを二値化したものをそのまま用いたが、例えば、カード所持者のサインを暗号化したものを用いたり、カード発行会社が独自の電子透かし情報をカード所持者に関わりなくカード発行

情報として埋め込んだり、また、PIN（個人認証番号）と電子透かし情報とが連動して初めてICカード認証システムが認証機能を開始するように設定することも可能である等、種々の変形実施が可能である。

【0064】また、本発明に係るICカードによれば、ICチップ11に記憶されている第1の認証情報と顔写真情報12に埋め込まれている第2の認証情報とは、照合することにより正当性を認証することが可能な情報であればよく、必ずしも同一情報としなくとも良い。これは、例えば、入退出管理等のように役職や資格等の種別により入退出の管理を行う場合、ICチップ11に従業員コード等の情報を記憶させ、顔写真情報12に該当する役職や資格を電子透かし情報として埋め込み、入退出の制限をICチップ11に記憶されている従業員コード等により社員か否かを判定し、さらに、顔写真情報12に電子透かし情報として埋め込んだ役職や資格により、その場所に入退出可能な人物か否かを判定するようにしても良い。

【0065】

【発明の効果】以上の説明より明らかなように、本発明に係るICカードによれば、ICチップに記憶されている第1の認証情報と顔写真情報等に埋め込まれている第2の認証情報とが、照合することにより正当性を認証することが可能な情報からなるため、改ざん及び偽造等の行為が行われた場合には、所定の読み出し装置により読

み出して確認することができ、また、顔写真等を見ただけではその顔写真等に電子透かし情報が埋め込まれていることを第三者が容易に知ることは困難である。従って、顔写真の改ざんやICチップに記憶された情報が書き換えられるといった偽造及び改ざん行為を企む、第三者を多に牽制することができる。

【0066】また、本発明に係るICカード認証システムによれば、偽造及び改ざん行為が行われたICカードが不正使用されているか否かを、上述した本発明のICカードのICチップや顔写真情報に記憶及び隠匿されている認証情報の判定に基づいて判断する。従って、偽造及び改ざんが成されたICカードであるか否かを容易に判別することができる。

【図面の簡単な説明】

【図1】本発明の実施形態であるICカードの外観を示す概略図である。

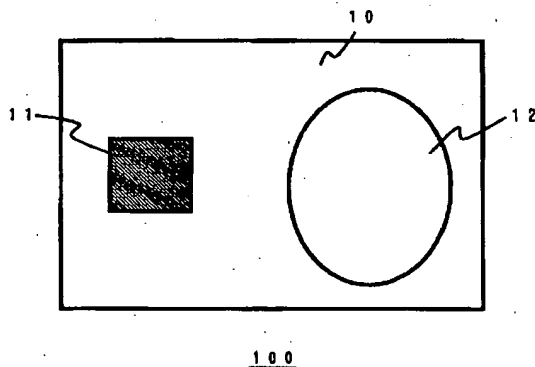
【図2】本発明の実施形態であるICカード認証システムの構成を示すブロック図である。

【図3】本発明の実施形態であるICカード認証システムの認証動作の一例を示すフローチャートである。

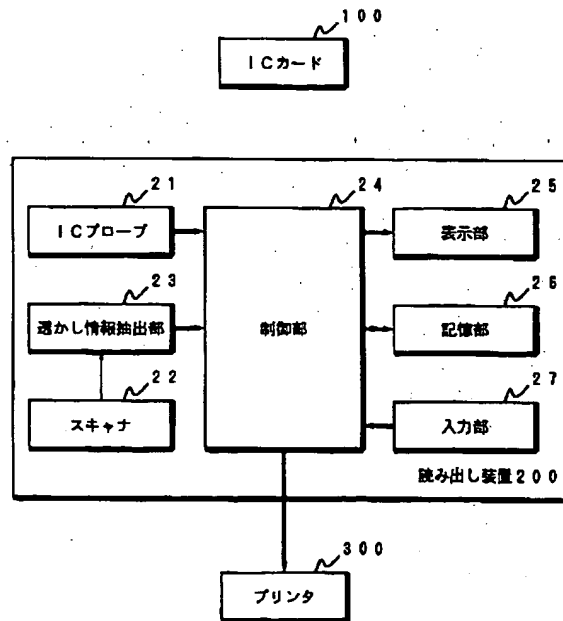
【符号の説明】

- 1 カード基材
- 11 顔写真情報
- 12 ICチップ
- 100 ICカード

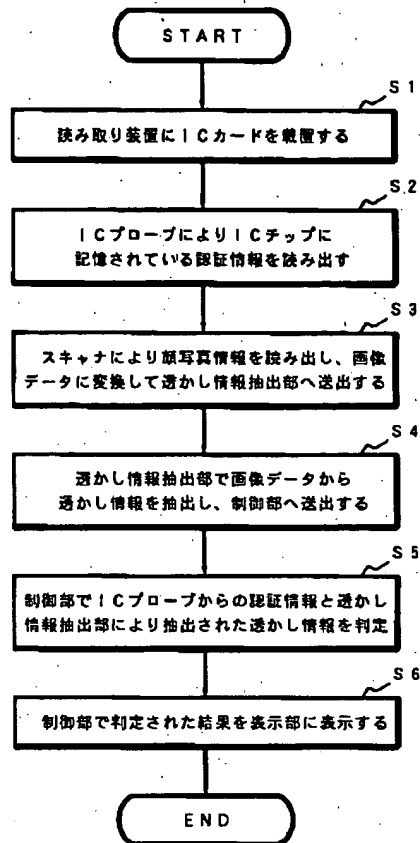
【図1】



【図2】



【図3】



フロントページの続き

(51) Int. Cl. 7

G 0 9 C 1/00

5/00

H 0 4 N 1/387

識別記号

6 6 0

F I

H 0 4 N 1/387

G 0 6 K 19/00

テーマコード(参考)

5 J 1 0 4

R 9 A 0 0 1

F

Fターム(参考) 2C005 MA03 MA04 MB01 MB08 MB10

SA14

5B035 AA15 BB09 BB11 CA38

5B057 AA20 BA24 CA01 CA06 CA08

CA16 CA19 CB01 CB06 CB08

CB16 CD03 CE08 DA16 DB06

DB08 DB09 DC32

5B058 CA16 KA02 KA05 KA06 KA38

5C076 AA14 AA24 BA03 BA04 BA06

CA02 CA08

5J104 AA07 AA14 KA01 KA16 NA13

NA14 NA15 NA35 NA38

9A001 BB05 BB06 HH23 LL03